CALIFORNIA STATE THREAT ASSESSMENT CENTER

24-HOUR REPORT

21 SEPTEMBER 2017

(U) CALIFORNIA

(U) San Francisco – Hackers Used Avast CCleaner Breach to Attack Technology Companies
(U) The hackers who broke into widely used computer utility software in August also tried to infect machines at Microsoft, Intel, and other top technology companies, according to research by Cisco Systems released late yesterday. That suggests the breach, disclosed on 18 September, was far more serious than initially described by Piriform, maker of the infected CCleaner utility and now a part of Prague-based Avast Software. Researchers at Cisco, one of the companies that had warned Avast of the attack, said that a control server seized by US law enforcement showed that the hackers had installed additional malicious software on a selected group of at least 20 machines at major technology companies.
SOURCE: 20 September 2017, Reuters

(U) NATIONAL

(U) New York – $30 Million Worth of Illicit Fentanyl Recovered in Record-Breaking Bust
(U) New York City – Police in New York City are being credited with getting millions of dollars in drugs off the streets in a record drug bust. Four people are under arrest after authorities seized 270 pounds of narcotics, including 140 pounds of pure fentanyl with a street value of over $30 million. The record-breaking amount of fentanyl was discovered at a residential building in Queens, as well as 213 pounds of other narcotics like cocaine and heroin that had been laced with fentanyl. Meanwhile in the Bronx, authorities say they seized 55 pounds of fentanyl and heroin from a stopped vehicle. Authorities say they recovered 25 brick sized packages, each weighing a little over two pounds, inside the stopped vehicle.
SOURCE: 20 September 2017, WDSU News

(U) New York – SEC Reveals It Was Hacked, Information May Have Been Used for Illegal Stock Trades
(U) New York City – The Securities and Exchange Commission, the country's top Wall Street regulator, announced yesterday that hackers breached its system for storing documents filed by publicly traded companies last year, potentially accessing data that allowed the intruders to make an illegal profit. The agency detected the breach last year, but did not learn until last month that it could have been used for improper trading. The system that was breached, known as EDGAR, is a popular way for investors to access the detailed financial reports companies that sell stock to the public must periodically release. The breach did not lead to the release of personally identifiable information, but may have provided the basis for illicit gain through trading. An investigation into the matter is ongoing.
SOURCE: 20 September 2017, The Washington Post

(U) INTERNATIONAL

(U) France – ISIS Backers Find Ephemeral Platform on Instagram
(U) Paris – Researchers say Islamic State of Iraq and ash-Sham (ISIS) supporters have found an ephemeral platform to share propaganda: using Instagram's "stories" feature, which causes posts to

disappear in 24 hours. The software analysis identified more than 50,000 accounts linked to ISIS supporters posting Instagram stories, according to the software research group Ghost Data. Of those 50,000, just over 10,000 are described as strongly-linked to ISIS—they follow core ISIS accounts and are followed back, and about 30 percent of their posted content is about the group. There is no sign that the majority of the posts are from ISIS's central propaganda units—rather, they tend to be personal snapshots with little production value, like a clip of the ISIS trademark black flag or a photo showing what happens to "traitors."
SOURCE: 20 September 2017, Associated Press

(U) Iran – Security Expert Report Iran Cyber-Espionage Capabilities Have Increased
(U) Tehran – Hackers probably linked to Iran's government have hit Saudi and Western aerospace and petrochemical firms, marking a rise in Iranian cyber-spying prowess, security firm FireEye said yesterday, an assessment shared by other US experts. A FireEye report dubbed the hacker group APT33 and offered evidence of its activities since 2013 in seeking to steal aviation and military secrets, while also gearing up for attacks that might cripple entire computer networks. In a separate but related move last week, the US Treasury Department added two Iran-based hacking networks and eight individuals to a US sanctions list, accusing them of taking part in cyber-enabled attacks on the US financial system. Several cyber experts described rising maturity and professionalism in Iran's cyber-espionage capabilities.
SOURCE: 20 September 2017, Reuters

(U) Malaysia – Authorities Arrest Seven Suspected of Involvement with Abu Sayyaf Group
(U) Kuala Lumpur – Malaysia arrested seven Philippine men suspected of involvement in activities of the Abu Sayyaf militant group, police said today, as concern grows in Southeast Asia over the possible expansion of extremist activity. Abu Sayyaf, whose members have pledged loyalty to ISIS, is notorious for bombings, beheadings, extortions, and kidnap-for-ransom activities in the Philippines' south. The men worked as security guards for private companies in the capital, Kuala Lumpur, and the surrounding state of Selangor. Malaysian police said their arrests were based on information received after authorities thwarted a plan by an Abu Sayyaf member to stage an attack at the closing ceremony of the Southeast Asian Games in Kuala Lumpur last month.
SOURCE: 20 September 2017, Reuters

(U) Mexico – Gunman Kill Two State Investigators, Child at Shopping Center Frequented by Tourists
(U) Cancun – Authorities in the Mexican resort city of Cancun say gunmen have killed two agents who were investigators for the state prosecutor's office, as well as a child who was with them. The investigators were in the parking lot of the Gran Plaza shopping center when they were shot on 16 September, their day off. The male victim was a commander who had received threats recently and was believed to be targeted because of his work against cartel activities. More than 120 executions have been registered in the Mexican state of Quintana Roo so far this year, 13 of them just in the month of September.
SOURCE: 18 September 2017, Yucatan Times

(U) United Kingdom – Authorities Arrest Sixth Suspect in Train Attack
(U) London – Police have arrested a 17-year-old boy in south London in connection with the 15 September terror attack on a District Line train at Parsons Green which injured 30 people. The teenager was detained after officers executed a warrant in Thornton Heath today. It takes the total number of arrests in the investigation to six, all of whom remain in custody at a south London police station.
SOURCE: 21 September 2017, BBC News

(U) PREPARED BY THE CALIFORNIA STATE THREAT ASSESSMENT CENTER.

(U) FOR QUESTIONS OR CONCERNS, PLEASE EMAIL STAC@CALOES.CA.GOV, OR CALL 916-874-1100.

This document contains excerpts of suspicious activities and incidents of interest to the STAC as obtained from open and unclassified sources.